

EXPRESS MAIL NO. EV 286 259 339 US

Docket No. 03AB086

Q&B Ref: 110003.00035

**PATENT APPLICATION FOR
SAFETY CONTROLLER PROVIDING RAPID
RECOVERY OF SAFETY PROGRAM DATA**

By

**Joseph Paul Izzo
Norman Sievert Shelvik
Michael Dean Kalan
Charles Martin Rischar
Raymond Louis Buvel**

SAFETY CONTROLLER PROVIDING RAPID
RECOVERY OF SAFETY PROGRAM DATA

CROSS-REFERENCE TO RELATED APPLICATIONS

[0001] --

STATEMENT REGARDING FEDERALLY
SPONSORED RESEARCH OR DEVELOPMENT

[0002] --

BACKGROUND OF THE INVENTION

[0003] The present invention relates to industrial controllers used for real time control of industrial processes, and in particular to “high reliability” or “safety” industrial controllers appropriate for use in devices to protect human life and health.

[0004] Industrial controllers are special-purpose computers used in controlling industrial processes. Under the direction of a stored control program, an industrial controller examines a series of inputs reflecting the status of the controlled process and changes a series of outputs controlling the process. The inputs and outputs may be binary, that is, on or off, or analog, providing a value within a substantially continuous range. The inputs may be obtained from sensors attached to the controlled process, and the outputs may be signals to actuators on the controlled process.

[0005] “Safety systems” are systems intended to ensure the safety of humans working in the environment of an industrial process. Such systems may include the electronics associated with emergency-stop buttons, light curtains, and other machine lockouts. Traditionally, safety systems have been implemented by a set of redundant circuits separate from the industrial control system used to control the industrial process with which the safety system is associated. Such safety systems have been “hardwired” from switches and relays including specialized “safety relays” which provide comparison of redundant signals and internal checking of fault conditions such as welded or stuck contacts.

[0006] Hard-wired safety systems using duplicate wiring have proven cumbersome in practice in part because of the difficulty of installing and connecting

hardwired components and duplicate sets of wiring, particularly in complex control applications, and in part because of the difficulty of troubleshooting and maintaining a hard-wired system whose logic can be changed only by re-wiring.

[0007] For this reason, there has been considerable interest in developing industrial controllers that may implement safety systems using a program simulating the operation of the physical components in hard-wired safety systems. Industrial controllers are not only easier to program but can provide reduced installation costs by eliminating long runs of redundant wiring in favor of a high speed serial communication network and by providing improved troubleshooting capabilities.

U.S. Patent applications 60/373,592 filed April 18, 2002; 10/034,387 filed December 27, 2001; 09/667,145 filed September 21, 2000; 09/666,438 filed September 21, 2000; and 09/663,824 filed September 18, 2000, assigned to the assignee of the present invention, describe the implementation of safety systems using industrial controller architectures, and are hereby incorporated by reference.

[0008] Establishing the necessary degree of reliability for safety controller hardware and operating system software can be done by careful attention to the design of this hardware and software. Establishing this reliability for the control program executed by the controller, however, is more difficult. The control program is normally written by the user for a specific application on an application-by-application basis. Further, the control program may be prepared on a common desktop computer using a standard commercial operating system and other software whose configuration and reliability cannot be easily verified and which is outside of the control of the safety controller manufacturer.

[0009] For this reason, each control program must be individually certified after it is loaded into the safety controller. This certification step involves operating the control program in a test environment and confirming that the correct outputs are generated during a simulated operation of the safety system. After completion of the certification process, the control program may be run.

[0010] In the event that the safety program as stored in the safety controller is lost and must be recovered from the external desktop computer or the like, or edited using the desktop computer, the certification of the control program is lost and the

certification process must be repeated, a costly and time consuming operation. In complex control programs where both safety tasks and standard tasks are executed on the same controller, the need to edit the control program is common.

SUMMARY OF THE INVENTION

[0011] The present invention provides a safety controller that may readily establish that safety portions of the control program, such as may be downloaded from an external computer, are identical to a previously downloaded and certified version of the program. In this way, the need for re-certification is avoided. The invention may distinguish between standard program tasks and safety tasks to ignore changes in the standard tasks, allowing standard tasks to be freely edited without the need for re-certification of the safety tasks.

[0012] Specifically, the present invention provides a safety controller that may execute a safety program and operate according to a stored program to download safety program data to a memory of the controller. A signature is derived from the safety program data in memory, the signature being functionally dependent on values of the safety program data in memory. The signature is then compared to a stored signature derived from a previously certified safety program data.

[0013] It is thus one object of the invention to simply establish whether a reloaded safety program data is identical to safety program data that has been previously certified so as to avoid the need for re-certification.

[0014] After certification, the controller may upload a representation of the safety program data as stored in memory.

[0015] It is thus another object of the invention to provide a convenient version of the safety program data that may be stored externally for safekeeping by a user. It is another object of the invention to provide a version of the safety program data that, when correctly re-downloaded, produces the same signature as the originally certified data.

[0016] The controller may store a copy of the representation of the safety program data as stored in memory in a separate portion of memory. This portion of memory may be non-volatile.

[0017] Thus it is another object of the invention to allow rapid recovery of the safety program data in the event of power loss without the need to re-download the safety program data from an external source.

[0018] The safety industrial controller may block execution of the safety program in memory when the derived signature does not match the stored signature.

[0019] Thus it is another object of the invention to prevent corrupted safety program data or safety program data that has not been certified, from being executed.

[0020] On the other hand, the program may allow execution of the safety program in memory when the safety program data is specifically indicated not to have been previously certified.

[0021] Thus it is an object of the invention to allow freedom in downloading new safety program data for the purpose of initial certification.

[0022] The controller may provide an output indication to a user when the derived signature does not match the stored signature.

[0023] Thus it is another objection of the invention to invoke human oversight in possible failures of the signatures to match.

[0024] The controller may further output the signature to a user for recordation.

[0025] It is another object of the invention to provide the signature to the user to be used to distinguish among competing certified versions of the program.

[0026] The safety program data may include executable instructions and data providing arguments to the executable instructions.

[0027] Thus it is another object of the invention to provide assurance that both the executable instructions and the initial values of data used by those instructions are identical to that which was certified.

[0028] The signature may be derived using a cyclic redundancy code taking safety program data as an argument.

[0029] It is thus another object of the invention to provide a highly compressed signature using techniques well characterized in the art to provide extremely low possibilities of undetected differences between the safety program data and the previously certified safety program data.

[0030] The signature may be functionally independent of standard program data also received by the controller.

[0031] Thus it is another object of the invention to permit editing of non-safety or "standard" portions of a control program when the safety controller executes both safety tasks and standard tasks, where the standard tasks are those which do not require as high a degree of reliability as required by the safety tasks.

[0032] The safety industrial controller may provide two processors having associated portions of memory and the controller may download the safety program into both portions of memory and use the safety program in both portions of memory to derive a signature functionally dependent on both portions. The stored signature used in the comparison may be from previously certified safety program data executed on the controller in both portions of memory.

[0033] Thus it is another object of the invention to provide a system that works with redundant controllers used to provide high reliability.

[0034] These particular objects and advantages may apply to only some embodiments falling within the claims and thus do not define the scope of the invention.

BRIEF DESCRIPTION OF THE FIGURES

[0035] Fig. 1 is a simplified perspective view of a controller system suitable for use with the present invention, including a primary and partner controller communicating on a backplane 26 and a programming terminal communicating with the primary controller on a dedicated interface;

[0036] Fig. 2 is a block diagram of the memories of the programming terminal, the primary controller, and the partner controller, showing stored operating systems, safety and standard control tasks, and a snapshot and signature of the safety tasks;

[0037] Fig. 3 is a flowchart showing execution of the operating systems of the primary and partner controllers in downloading safety and standard tasks into the primary and partner controllers and the generation of a snapshot and signature of the safety tasks;

[0038] Fig. 4 is a flowchart showing the steps of recovery of the program data or of new edited data using the snapshot and signature.

DETAILED DESCRIPTION OF THE PREFERRED EMBODIMENT

[0039] "High reliability" and "safety" systems are those that guard against the propagation of erroneous data or signals by detecting error or fault conditions and signaling their occurrence and/or entering into a predetermined fault state. High reliability systems may be distinguished from high availability systems which attempt to remain operating after some level of failure. The present invention may be useful in both systems, however, and therefore, as used herein, high reliability and safety should not be considered to exclude high availability systems that provide safety operation.

[0040] Referring now to Fig. 1, a dual controller safety system 10 suitable for use with the present invention, provides a chassis 12 into which a set of control modules 14 may be inserted according to the particular control application. Each of the modules 14 provides an electrical connector at its rear, not shown, that may connect with a corresponding connector on the front surface of a backplane 26 forming the rear wall of the chassis 12. The connectors are joined by conductive traces so that the modules 14 may be freely inserted into the chassis 12 to intercommunicate on the backplane 26 according to methods well known in the art.

[0041] The control modules 14 may include, generally, a power supply 16, a network module 20, a primary controller 18a, a partner controller 18b, and one or more I/O modules 22. The power supply 16 may provide a source of regulated power over power conductors of the backplane 26 to the other control modules 14 while the network module 20 provides a connection between the backplane 26 and a high speed serial network 34 such as Ethernet or the like. The network 34 may communicate with a remote chassis, not shown, having other I/O modules and controllers. Both the backplane 26 and the network 34 and the interfaces thereto may support a safety protocol such as described in U.S. Patent Application 60/373,592 referenced above.

[0042] The I/O modules 22 may communicate with various sensors and actuators, not shown, of a control process 40. The control process 40 may include standard processes such as those controlling factory equipment or the like and safety processes related to safety applications.

[0043] In the preferred embodiment, the primary controller 18a and the secondary controller 18b are contained in separate housings, each independently attachable to the backplane 26 of the chassis 12. Each of the primary controller 18a and the partner controller 18b provide an independent processor and memory for executing a control program. The primary controller 18a includes a serial communication port providing a serial link 30 to a programming terminal 32. The programming terminal 32 may be a standard PC-type computer.

[0044] Referring also to Fig. 2, memory 42 of the terminal 32 may hold an operating system 44 such as the Windows operating system manufactured by Microsoft Corporation. The terminal 32 may also hold and execute standard programming tools 46 for generation of control programs, for example, using relay ladder logic or the like. The programming tools 46 may be used to generate safety tasks 48 and standard tasks 50, the former addressing the safety processes of control process 40 and the latter addressing the standard processes of control process 40. Generally the standard tasks 50 will accept a lower degree of reliability than the safety tasks 48. As used herein, the task 48 and 50 include both executable program instructions and data values. The programming tools 46 are modified from those normally used so that each generated task 48 and 50 is identified as to whether it is a safety task 48 or a standard task 50 using an embedded file header or the like.

[0045] Referring now also to Fig. 3, after the creation of the safety tasks 48 and standard tasks 50 in the programming terminal 32, as indicated by process block 52, the safety tasks 48 and standard tasks 50, together comprising a control program, are downloaded over serial link 30 to the primary controller 18a and the secondary controller 18b per process block 54. In the preferred embodiment, the safety tasks 48 are executed on both controllers 18a and 18b and the execution by each of the controllers 18a and 18b is periodically compared to ensure that a failure of either has not caused an error in the execution of the control program on one device. The standard tasks 50 in contrast may be loaded onto a single controller for execution there. The operation of the controllers 18a and 18b is described in detail in co-pending application entitled Safety Controller Providing for Execution of Standard and Safety Control Programs, filed September 16, 2003.

[0046] The primary controller 18a has a memory 56 and the partner controller 18b has a memory 58. Each of these memories 56 and 58 holds portions 60 and 62 of a controller operating system which provides for the execution of the invention, as will be described and which is particularly designed for high reliability operation.

[0047] As indicated by process block 54, identical copies of the safety tasks 48 are loaded into a first safety area 64 of memory 56 and safety area 66 of memory 58, as indicated by arrows 70. In contrast, the standard tasks 50 are loaded into standard area 72 of memory 56 only. Generally as described above, the safety tasks 48 in safety memory areas 64 and 66 will execute *in tandem* and compare their execution to detect possible hardware or software failures, whereas the standard tasks will execute only on controller 18a.

[0048] Referring again to Fig. 3 as indicated by process block 74, once the tasks 48 and 50 are loaded into the primary controller 18a and partner controller 18b, the user may certify the safety portions of the control program, comprised of the safety tasks 48 in safety memory areas 64 and 66, by executing those portions and testing their operation using test procedures understood in the art. The downloaded control program will not be associated with a signature, as will be described below, and thus may be executed with the appropriate warning to the user that the program is not certified. This will also be true if the control program was not downloaded, but was edited on-line, a process which will erase the signature.

[0049] Upon completion of the certification, the user may send an instruction from the terminal 32 to the controllers 18a and 18b causing generation of snapshots 82 and 84 of the safety tasks 48 in the safety memory areas 64 and 66. Specifically, a memory image of safety memory areas 64 and 66 is copied to snapshot areas 78 and 80 of memories 56 and 58, respectively, to produce a snapshot 82 and 84. This copying is indicated by arrows 86 and 88.

[0050] A memory image generally preserves the ordering of the data of the safety tasks 48 according to the absolute memory address ordering in the safety memory areas 64 and 66. Note that generally, the safety tasks 48 will load differently into safety memory areas 64 and 66 to produce different memory images and that different memory images will be produced on subsequent loadings of the

safety tasks into safety memory areas 64 and 66 depending on a number of factors, including the order in which the safety tasks are downloaded. The snapshots 82 and 84 will thus be unique to the particular circumstances of the downloading and, in general, will differ from each other.

[0051] At process block 79, a signature 90 and 92 respectively, is then created from each snapshot 82 and 84. The signatures 90 and 92 are generated by using a cyclic redundancy code ("CRC") which provides, in essence, a highly compressed 32 bit integer representing each snapshot 82 and 84 and providing a probability of less than 2×10^{-9} of a different snapshot providing the same signature. Attached to the CRC is a date and time value, which together with the CRC comprises the signatures 92 and 90. The CRC polynomials used may be selected from a variety of different polynomials but in the preferred embodiment are standard Ethernet polynomials.

[0052] A second CRC algorithm produces a single global signature 94 by combining the signatures 90 and 92 for each of the snapshots 82 and 84.

[0053] As indicated by process block 96, the signatures 90 and 92 are attached to the snapshots 82 and 84, the package is then attached to the global signature 94 and uploaded to the terminal 32. Generally, the terminal 32 may hold several uploaded snapshots of different times and dates. As indicated by process block 98, the global signature 94 is displayed visually to the user who may copy it down manually for a positive identification of the program version represented by the uploaded snapshot. At this time, the control program may be freely executed without warning to the user.

[0054] Referring now to Fig. 4 and Fig. 2, the safety task 48 in safety memory areas 64 and 66 may be lost through power failure or damage or the like. In the case of power loss, the snapshots 82 and 84, as indicated by process block 106, as held in non-volatile memory, may be used to quickly re-establish the safety tasks 48. In the case of loss or damage to the snapshots 82 and 84 or where it is desired to revert to a previously certified version, a new snapshot is downloaded from the terminal 32 to the snapshot areas 78 and 80 as indicated by process block 102. The particular snapshot to be downloaded is selected by the user.

[0055] At process block 108, derived global signature 94 computed from the snapshots 82 and 84 is compared to the stored global signature 94 stored as part of the downloaded or stored snapshots 82 and 84. If they do not match, the program moves to a stop state 110 where the user is notified of the failure of the matching and execution of the control program is prevented.

[0056] If, on the other hand the signatures 94 match, then the global signature is uploaded to the user who may compare it against a written copy to ensure that the latest version of the snapshots 82 and 84 have been downloaded as indicated by process block 112. If the user approves of the signature per process block 114, then at process block 116, the snapshots 82 and 84 are unpacked into safety areas 64 and 66 and execution may begin.

[0057] It is specifically intended that the present invention not be limited to the embodiments and illustrations contained herein, but include modified forms of those embodiments including portions of the embodiments and combinations of elements of different embodiments as come within the scope of the following claims.